Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

040.101 Application Backup Policy

Version 2.1
September 14, 2018

Revision History

Date	Version	Description	Author
12/13/2006	1.0	Effective Date	CHFS IT Policies Team Charter
9/14/2018	2.1	Review Date	CHFS OATS Policy Charter Team
9/14/2018	2.1	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive (or designee)	9/14/2018	Jennifer Harp	Jennifer K. Harp
CHFS Chief Information Security Officer (or designee)	8/20/2018	DENNIS E. LEBER	D. E. L

Table of Contents

1 Policy Definitions

- **Availability:** The reliability and accessibility of data and resources to authorized individuals in a timely manner. The security objective that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.
- **Confidentiality:** A security principle that works to ensure that information is not disclosed to unauthorized subjects (people, systems, or devices). The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.
- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Data Classification- NIST High Impact Level:** Severe or catastrophic effect on organizational operations, organizational assets, or individuals resulting in severe degradation to or a complete loss of an organization’s ability to carry out its mission, severe financial loss, and/or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
- **Data Classification- NIST Moderate Impact Level:** Serious adverse effect on organizational operations, organizational assets, or individuals including resulting in significant degradation to an organization’s ability to carry out its mission, significant financial loss, and/or significant but non-life-threatening harm to individuals.
- **Data Classification- NIST Low Impact Level:** Limited adverse effect on organizational operations, organizational assets, or individuals resulting in minor degradation to an organization’s ability to carry out its mission, minor financial loss, and/or minor harm to individuals.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.

- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual's tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.
- **Integrity:** A security principle that ensures information and systems are not modified maliciously or accidentally. The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual's personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother's maiden name, etc.).
- **Recovery Point Objective (RPO):** The age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure.
- **Recovery Time Objective (RTO):** The targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **System/Data Administrator:** An individual who is responsible for the data administration process by which data is monitored, maintained, and managed. This person is responsible for controlling application data assets, as well as their processing and interactions with different applications and business processes. This person is also tasked with access management to the system/data using the Role-based Access Control (R-BAC) model. In the Cabinet for Health and Family Services this role is generally played by a CHFS Branch Manager.

- **System/Data Custodian:** An individual who is responsible for the maintenance and protection of the data. This role is usually filled by the IT department, which owns the Infrastructure. The duties include performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in the enterprise security policies, standards, and guidelines that pertain to information security and data protection. In the Commonwealth of Kentucky this role is generally played by Commonwealth Office of Technology (COT).
- **System/Data Owner:** The person who has final agency responsibility of data protection and is the person held liable for any negligence when it comes to protecting the specific application's data/information assets. This role/person is the owner of the system that holds the data, usually a senior executive, designates the confidentiality of the system/data, and assigns the data admin, and dictates how the information should be protected based on business' policies. In the Cabinet for Health and Family Services this role is generally played by a CHFS Business Executive.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through an application backup policy. This document establishes the agency's Application Backup Policy that helps manage risks and provides guidelines for security best practices regarding system backups. To minimize the possible disruption to business operations, CHFS shall establish and maintain an effective schedule for the backup of critical data.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with organizations and/or agencies with the cabinet, which access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible to adhere to this policy.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section 8 Policy References below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who work with the application's development team to document components that are not included in the base server build and ensure functionality and backups are conducted in line with business needs. This individual(s) will be responsible to work with enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

4 Policy Requirements

4.1 Data Backup

CHFS information technology system's data, deemed critical, are required to be backed-up on a regularly scheduled basis for continued operation of critical functions.

CHFS data and backups that have regulatory or compliance requirements, containing ePHI/PHI/PII/HIPPA/FTI/SSA/Sensitive data, shall be encrypted in transit and at rest. CHFS agencies that seek exception(s) to encryption of data and backups in transit or at rest must follow guidance and obtain approval established in the CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy. Data at rest includes data stored in the database, backup archive files, folder, file systems, and removal media. Backups shall never leave the United States; refer to CHFS 020.301 CHFS Network User Accounts Policy.

COT is responsible to perform the application data/backups on CHFS hosted applications, while vendors are responsible for the application data/backups of non-CHFS hosted applications. COT and vendors shall be responsible for:

a. Providing adequate operational resources for data backup and testing of media.
b. Instructing appropriate staff in data backup and recovery procedures.
c. Ensuring the data backup and recovery procedures are followed.
d. Ensuring that only authorized people with sufficient knowledge conduct the backup and recovery processes.
e. Ensuring that all state and federal regulations are in compliance during the backup and recovery processes.

The CHFS agency System Data Owner and/or the System Data Administrator is responsible for the backup, archival, and retention of paper documents (i.e. files, records, etc.). The CHFS agency shall follow applicable federal and state laws, regulations, and guidelines when handling paper archival documents.

4.2 Data to be Backed-up

All data needed to return an inoperable application to a normal state shall be backed up. By default, COT only backs up operating system files. System Data Owner and/or the System Data Administrator must request COT to back up specific data.
Examples include, but are not limited to, the following:

- All configuration settings applicable to an application's functionality.
- All data deemed critical as defined by application owners.
- All applications' user accounts or key information related to accessing the application.

4.3 Backup Frequency

Backup frequency is critical to successful data recovery. In determining the backup frequency, the System Data Owner and/or the System Data Administrator must determine the Recovery Point Objective (RPO).

4.4 Backup Storage

Data/Application backups typically contain confidential information and, as such, precaution must be taken to ensure the security and integrity of the data and the medium on which that data resides. On-site and off-site storage must be in a secure, access-controlled area and must use accepted methods of environmental controls to include fire suppression.

4.5 Backup Retention

Backup and retention schedules are based on the criticality of the data being processed and the frequency in which that data is modified. System Data Owner and/or the System Data Administrator are responsible for working with COT for file and log backup retention schedules to meet necessary business requirements, NIST 800-53 Revision 4 compliance, CHFS Records Retention Schedule, Kentucky Department for Libraries and Archives (KDLA), as well as applicable federal and state regulations.

4.6 Backup Restoration Procedures and Testing

System Data Owner and/or the System Data Administrator shall have restoration procedures documented and tested. Documentation must include, but is not limited to, the following:

- Responsible party to approve a restore;
- Process followed to restore;
- Under what circumstances it is to be performed;
- Time required from request to restoration;
- Defined acceptable Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Backup restoration testing, (i.e. full application functionality test, smoke testing, operations readiness and assurance testing, etc.) must be performed at least one (1) time a year and when any change is made that may affect the backup system(s). Results of the restoration tests shall be documented by the System Data Owner and/or the System Data Administrator and available upon request.

Although the agencies System Data Owner(s) are responsible for defining the duration of onsite versus offsite storage, restoration documentation and test results must be retained for at least ten (10) years in accordance with the CHFS Records Retention Schedule, Kentucky Department for Libraries and Archives (KDLA) requirements.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS Records Retention Schedule, Kentucky Department for Libraries and Archives (KDLA)
- Enterprise IT Policy: CIO-058 IT Equipment Room Access at the Commonwealth Data Center Policy
- Enterprise IT Policy: CIO-059 Equipment Installation and Removal at the Commonwealth Data Center Policy
- Enterprise IT Procedure: COT-009- Change Management Procedure
- Enterprise IT Procedure: COT-067- Enterprise Security Standard Process and Procedure Manual (ESPPM) Process
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information